Saving Lives and Property Through Improved Interoperability

Wireless Data Standards and Technology Report

SUMMARY REPORT (3)

Final

May 2003

1. INTRODUCTION

As an adjunct to existing voice radio systems that are used for routine communications, public safety agencies are continuing to deploy new and innovative wireless data (i.e., non-voice) communications systems. Wireless data communications offer an additional form of communications to support the varied mission requirements of public safety organizations. Further, wireless data communications offers another avenue of interoperability benefits that extend past the internal unit-to-unit transfer of information within agencies. In fact, depending on the application, several wireless data technologies may provide multiple, disparate agencies with the ability to communicate vital information pertaining to a multi-agency response in real time. The Public Safety Wireless Network (PSWN) Program continues to explore advancements in wireless data communications that are capable of providing seamless, integrated public safety communications.

This report focuses on those efforts that are either currently being implemented or are being considered by public safety agencies across the globe. The *Wireless Data Networking Standards Support Report* is comprised of the following sections:

- **Section 1—Introduction.** This section provides an overview of the report.

- **Section 2—Previous and Future Reports**. This section provides a chronicle of the topics presented in the previous wireless data networking standards reports and gives a general overview of each topic. Additionally, this section addresses Wireless Data Standards and Technology Reports to be studied in the future.
    - i-mode/mMode
    - 802.11
    - Intelligent Transportation Systems
    - Biometrics
    - 802.20

- **Section 3—Technology Reports.** This section includes two "white papers" describing advancements in wireless data technologies and standards.
    - Wearable Computers
    - Wireless Emergency Warning Via Cell Broadcast

2. PREVIOUS AND FUTURE REPORTS

In the previous installments of the Wireless Data Networking Standards Support Reports, technologies and standards were presented. This section provides a chronicle of the topics presented in the previous reports and gives a general overview of each topic. Additionally, this section addresses Wireless Data Standards and Technology Reports to be studied in the future. For more detailed information on the below topics (excluding 802.20), please refer to the previous Wireless Data Networking Standards Support reports.

2.1 i-mode/mMode

Third generation (3G) wireless communication technology refers to pending improvements in wireless data and voice communications through any of a variety of proposed wireless standards. The immediate goal of 3G technology is to raise average data transmission speeds from current speeds of approximately 9.5 kilobits/second (kbps) to upwards of 2 megabits/second (mbps). This increase in data transmission rate will enable a 3G device to provide an extensive range of new functionality to mobile phone users. Until recently, mobile telephones have mainly been used for voice communications, voice messaging, as well as sending/receiving short message service (SMS) text. 3G will build on the current uses of the mobile telephone to offer simultaneous transfer of speech, data, text, pictures, audio, and video. The commercial cellular data services i-mode and mMode, both featured in this report, provide these enhanced services. Looking forward, 3G technology may revolutionize the way people use mobile devices; for example, it is envisioned that users will be able to shop online, perform online banking, or even play interactive games over the Internet using a handheld device.

The new 3G wireless systems will provide users a wireless link to a wide range of telecommunication services. Some of the key features of 3G systems include design consistency, compatibility of services, use of small wireless devices with worldwide roaming capability, Internet and other multimedia applications, and a wide range of value-added services. 3G technology, while already becoming increasingly widespread in usage and popularity in other parts of the world (e.g., Europe, Asia), is expected to reach maturity in the United States between 2003 and 2005. Some of the key service features and capabilities expected of 3G technologies are listed in Table 1.

Table 1
3G Service Features and Capabilities

3G Service Capabilities	Description
Circuit and packet data bit rates	• 144 kbps or higher in high mobility (vehicular) traffic • 384 kbps for pedestrian traffic • 2 Mbps or higher for stationary indoor traffic
Interoperability and roaming	• Roaming capabilities throughout Europe, Japan, and North America • Compatible with most, if not all, popular communications modes (e.g., Cellular, e-mail, paging, fax, videoconferencing, and Web browsing)

3G Service Capabilities	Description
Multimedia services and capabilities	• Fixed and variable data speeds depending on Internet traffic • Bandwidth on demand • Asymmetric data rates in the forward and reverse links • Enhanced multimedia (e.g., Voice, data, and remote control) • Broadband Internet access up to 2 Mbps

3G wireless technology will drive the future developments in mobile communications for both the consumer and business communities. 3G is expected to offer an "always-on" connection for users in most places. With the rapid growth of subscription wireless services in the United States, Europe, and elsewhere, carriers and infrastructure providers face the challenge of addressing bandwidth concerns resulting from this growth. Bandwidth limitations, coupled with the public's desire for always-on mobile wireless data services, have driven commercial service providers to develop technology solutions. This paper highlights two unique and relatively new commercial cellular data service solutions—i-mode and mMode. For a more detailed description of both i-mode and mMode 3G services, as well as an overview of the considerations for the application of these commercial wireless data services for the public safety community, please refer to Wireless Data Networking Standards Support Report – Summary Report (1).

2.2 802.11

Wireless local area networks (WLAN) are becoming increasingly common in the private sector, and some public safety agencies are actively using or considering the use of this technology. WLANs offer computers, handheld devices, and other wireless capable devices an always-on, mobile, wireless connection to each other, to local area networks (LAN), to wide area networks (WAN), and to the Internet. In addition, WLANs support connections to private intranets and virtual private networks (VPN).[1] A WLAN could facilitate the exchange of information between public safety personnel in and around facilities, between facilities, or potentially throughout a department's service area. The most recently approved standard, 802.11a, can potentially provide data transfer rates as fast as 54 megabits per second (Mbps).[2] As development of the technology progresses, data transfer rates may increase, products could become smaller, more powerful, and pervasive, and security features will likely be more robust. The benefits of WLANs may extend to improved employee timesaving and productivity efficiencies. However, as mobile data technology takes on a larger role in the day-to-day operations of public safety, those personnel charged with technology oversight are becoming increasingly burdened with keeping abreast of wireless technological advancements, implementation and support complexities, standards progression, and security requirements as they impact users.

1 A VPN is a private data network that uses the public telecommunication infrastructure, maintaining privacy using a tunneling protocol and security procedures.

2 *The peak data rate of 54 Mbps is based on the specifications of the IEEE standard for 802.11a.*

Although several standards-setting bodies are guiding the standards development process in a variety of technical areas, the Institute of Electrical and Electronics Engineers (IEEE), a non-profit, technical professional association, is leading the development of wireless connectivity standards. Officially titled "IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Networks," this suite of standards, more commonly referred to as 802.11, defines Ethernet WLANs. Specifically, the 802.11 suite of standards defines the "over-the-air interface" between the user's device and the base station or access points (AP) for a WLAN. As the standards development process progresses, additional protocols are introduced or altered to define certain characteristics, such as the physical layer (i.e., equipment) and security. An overview of the 802.11 standards investigated in this study is presented in the Table 2 below. For a more detailed description of the full 802.11 suite of standards, as well as an overview of the considerations for the application of 802.11 technology in the public safety community, please refer to Wireless Data Networking Standards Support Report – Summary Report (1).

Table 2
Comparison of Characteristics Specified within the IEEE 802.11 Suite

Characteristics	802.11	802.11a	802.11b	802.11g
Application	Wireless data networking	Broadband LAN Access	Wireless data networking	Broadband LAN Access
Spectrum Band	2.4 GHz UNII	5 GHz UNII	Unlicensed 2.4 GHz ISM	Unlicensed 2.4 GHz ISM
Modulation Scheme	FHSS or DSSS	OFDM	DSSS	OFDM or DSSS
Number of Channels	79 channels with FHSS; 3 or 6 channels with DSSS	12	3	3
Optimum Data Rates (Mbps)	2	54	11	54
Range (meters)	100	50	100	100
Date established (Market Ready?)	July 1997	September 1999	September 1999	January 2002—draft specification; final approval expected in June 2003
Compatibility	802.11 only	802.11a only	802.11g	802.11b
Operability	North America, Europe, Asia	North America, Europe, Asia	North America, Europe, Asia	North America, Europe, Asia

2.3 Intelligent Transportation Systems

In response to new political and economic constraints, transportation and public safety agencies are maximizing the efficiency of technology investments through cooperative efforts. These efforts enable joint acquisitions of technologies and facilities, and provide new information streams and capabilities that were previously unavailable. Transportation and public safety agencies are investing in new information and communication technologies that—

- Centralize traffic operations and public safety communications centers

- Deploy traffic and road condition monitoring systems
- Incorporate automatic vehicle location (AVL) systems and geographic information systems (GIS)
- Provide enhanced mobile information and communications systems for vehicle dispatch and status control.

To benefit from the potentially broad uses of these new information-sharing technologies and to improve the efficiency of transportation and emergency services, public safety and transportation agencies must work together in new ways by the sharing of informational assets, facilities, and communications infrastructure. Building new relationships between transportation and public safety entities is an important link in enhancing community safety. Regional, cross-agency, and cross-jurisdictional cooperation, along with jointly developed programs, plans, procedures, and technologies are fundamental to this effort. Detecting and effectively managing transportation incidents and efficiently sharing information with various emergency response agencies will decrease response times and reduce the impact on community health, safety, and commerce.

Intelligent Transportation Systems (ITS) encompass the application of advanced technologies and techniques such as communication systems, computers, electronics, and information processing in an integrated approach to improve the efficiency and safety of the nation's multimodal transportation network. ITSs improve the efficiency and effectiveness of the public safety services delivery through technological advancement in transit, traffic, and vehicle operations. Applying new information technologies to traffic and surface transportation incidents will improve detection, response, and recovery in emergencies. Table 3 below presents tasks and initiatives that are currently under development. For a more detailed description ITS initiatives and programs, as well as an overview of the considerations for the ITS technologies in the public safety community, please refer to Wireless Data Networking Standards Support Report – Summary Report (2).

Table 3
ITS Program Activities

Program Activity	Ongoing Tasks
ITS Public Safety Program	• Wireless Enhanced 911 (E911) summit and action plan • Wireless E911 deployment readiness • Wireless E911 technology innovation roundtable • Mayday/E911 Field Operation Test (FOT) • Integrated incident management FOT • Computer-aided dispatch (CAD)/ITS field FOT
Transportation Security	• New technology to secure cargo at U.S. ports • Request for Applications security model deployment • FY 03 ITS deployment program on security • Security workshops • Potential operational tests

Program Activity	Ongoing Tasks
Intelligent Vehicle Initiative	• Mack partnership generation zero FOT[3] • Pre-solicitation notice for Electronically Controlled Braking Systems (ECBS)[4] FOT • Drowsy driver warning system FOT • Minnesota snowplow project FOT • Naturalistic driving study
Metropolitan and Rural ITSs	• 511[5] travel information model deployment • State participation in 511 • Archive of user data service operational test solicitation • Variable Speed Limit (VSL)[6] FOT • Architecture conformity guidance document • Rural ITS strategic planning best practices document • Rural ITS toolbox document
Commercial Vehicle Information Systems and Network	• Commercial Vehicle Information Systems and Networks (CVISN)[7] Level 1 developments
Intermodal Freight	• Asset and cargo visibility test • Terminal dray[8] feasibility study
National ITS Architecture	• ITS deployment support • Turbo architecture • National ITS architecture evolution • National ITS architecture training

2.4 Biometrics

Every human being possesses more than one biological characteristic that can provide nearly infallible identification. The term "biometrics" has been coined to refer to the emerging field of technology devoted to the identification of individuals using biological traits. Biometrics examples include fingerprints, iris and retinal scans, hand geometry, and other measures of physical characteristics and personal traits. Technology has advanced biometrics to a highly automated process through which identification or verification occurs almost instantaneously.

---

[3] *Mack Partnership Intelligent Vehicle Initiative (IVI) Generation Zero FOT refers to the partnership of Mack Trucks and McKenzie Tank Lines with USDOT to evaluate the benefits of three IVI systems.*

[4] *ECBS benefits the trucking industry by dealing with the replacement of current brake application signals. This emerging technology will aid in the success of electronically controlled engines and transmissions. For further information, refer to the ITS Web site.*

[5] *On July 21, 2000, the Federal Communications Commission (FCC) assigned the 511 abbreviated dialing code on a national basis for the provision of transportation information. Further, the FCC ruling leaves it to state and local transportation agencies, telecommunications carriers, and regulators to determine the appropriate courses of action to make these services available. The USDOT ITS Joint Program Office is sponsoring an effort to document the progress of early implementers of 511 services for the benefit of the entire transportation community.*

[6] *VSL systems are sensory applications that help determine appropriate speeds for travelers, given current road and traffic conditions. The systems are used to reduce driver error and speeds, as well as to enhance roadway safety.*

[7] *CVISN Level 1 Developments deal with the electronic exchange of safety and credentialing information and electronic processing of interstate registration and fuel tax credentials, in addition to implementing roadside electronic screening at a fixed or mobile site.*

[8] *The terminal dray operations test will potentially improve cross-town movements of freight in Chicago, Illinois.*

Many definitions exist for the term biometrics, and although all the definitions are similar, each adds unique facets. According to the Biometric Consortium,[9] biometrics are "automated methods of recognizing a person based on a physiological or behavioral characteristic." A discussion paper entitled "Consumer Biometric Applications"[10] gives a more formal definition—a biometric is a "unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity."

Biometric applications, in general, were initially designed for wired use. However, with recent advancements in wireless data technology, biometrics are becoming feasible over the wireless medium. The main wireless advancements allowing for the wireless biometric applications are increased wireless data rates and bandwidths. This increase allows users to run real-time, data intensive applications wirelessly. Removing the dependence on wires will allow for more flexible biometric applications (e.g., scanning biometric information using handheld devices).

Some wireless biometric applications do not necessarily need increased bandwidth afforded by technological advances. In fact, some wireless biometric applications do not use the wireless medium at all. For example, biometrics can be used to authenticate a user for a specific wireless device, ensuring that only authorized personnel have access to that device. This is important for wireless devices that access sensitive or proprietary information. Many of these wireless devices give authorized users the ability to access information from behind enterprise firewalls (e.g., e-mail, personal or financial information). Use of biometrics augments sound wireless device security policies by making a wireless device useless to an unauthorized user.

Table 4 below presents different types of biometrics along with uses and characteristics of each. For a more detailed description of biometrics, as well as an overview of the considerations for biometrics technologies in the public safety community, please refer to Wireless Data Networking Standards Support Report – Summary Report (2).

Table 4
Comparison of Biometric Technologies[11]

Biometric	Use	Level of Robustness	Level of Distinctiveness	Level of Intrusiveness
Fingerprint	Identify or Verify	Moderate	High	Touching
Hand and Finger Geometry	Verify	Moderate	Low	Touching
Face	Identify or Verify	Moderate	Moderate	12+ inches
Voice or Speaker	Verify	Moderate	Low	Remote
Iris Scan	Identify or Verify	High	High	12+ inches
Retinal Scan	Identify or Verify	High	High	1-2 inches
Dynamic Signature Verification	Verify	Low	Moderate	Touching
Keystroke Dynamics	Verify	Low	Low	Touching

9 The Biometric Consortium is located at http://www.biometrics.org. The Biometric Consortium serves as the U.S. Government's focal point for research, development, test, evaluation, and application of biometric-based personal identification and verification technology.

10 "Consumer Biometric Applications: A Discussion Paper" is located on the Ontario, Canada, Web site of the Information and Privacy Commissioner at http://www.ipc.on.ca.

11 http://www.rand.org

2.5 802.20

On December 11, 2002, the IEEE Standards Board approved the formation of a working group to develop the IEEE 802.20 standard. The IEEE 802.20 Mobile Broadband Wireless Access (MBWA) specification is being developed as a standard to create an air interface that is optimized for the transport of Internet Protocol based services. The goal of the future standard, "Standard Air Interface for Mobile Broadband Wireless Access systems Supporting Vehicular Mobility – Physical and Media Access Control Layer Specification," is to enable worldwide deployment of affordable, ubiquitous, interoperable MBWA networks that boost real-time data transmission rates in wireless metropolitan area networks (MANs) for niche markets. The scope of the working group is to specify the physical and medium access control layers of the air interface for interoperable MBWA systems, operating in licensed bands below 3.5 GHz. The standard will address peak data rates per user in excess of 1 Mbps, deliver service levels to mobile users traveling up to 250 kilometers per hour in a MAN, and target sustained spectral efficiencies of more than 1 bit per second per Hertz per cell, giving users access to high-speed wireless data networks equivalent in quality to wired links. IEEE hopes to have the standard in place by the end of 2004. The IEEE 802.20 Working Group and specification will be explored in greater detail in a future Wireless Data Standards and Technology Report.

3. TECHNOLOGY REPORTS

During this reporting period, the PSWN Program has conducted research and developed two "white papers" discussing emerging data technologies and developing wireless data standards respectively, both of which may have significant impact on the public safety community. The information presented includes:

- **Wearable Computers.** The advantages offered by wearable computers are similar to those offered by portable computers, e.g., access to computers while away from the office or home; however, with the advancement of wearable computing technology, computing devices will provide hands-free interaction. This report highlights wearable computing technology, applications involved with wearable computers, as well as public safety applications.

- **Wireless Emergency Warning Via Cell Broadcast.** Cell broadcast has been identified as an effective way to wirelessly deliver emergency broadcast messages to large numbers of users in a localized area. This article presents an overview of cell broadcast technology and its applications within the public safety community.